

Re: is lavasoft recommended

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-05/2609.html>

From: Sandi – Microsoft MVP (sandi_hardmeier_at_mvps.org)

Date: 05/22/04

Date: Sat, 22 May 2004 20:10:21 +0800

Yes, with some provisos.

IMPORTANT: Before trying to remove spyware, download a copy of LSPFIX from the URL below – some malware can kill your internet connection when it is removed, and this software should get things going for you again:

<http://www.cexx.org/lspfix.htm>

IMPORTANT: After obtaining the software below, make sure you check for updates and then run the programmes in safe mode.

To be most effective, you must run AdAware while Windows is in safe mode, and you must shut down as many suspect processes as possible.

This can be tricky, but nothing is impossible. Modern malware uses more than one process, and these processes are 'co-dependent'. In other words, when one processes detects that the other has been shut down, it automatically restarts its sibling, often using a different name. Using Task Manager (ctrl, alt, del) doesn't work because you can only shut down one process at a time.

Disable suspect processes using MSCONFIG before booting into safe mode. Use the information at the URL below as a guide:

<http://www2.whidbey.com/djdenham/Uncheck.htm>

Then start AdAware. Make sure 'activate in depth scan' is enabled. Select 'use custom scanning options' and then click on the 'customize' button. Turn on the following scan options – scan within archives, active processes, registry (including deep scan), IE favorites and hosts file. You must also turn on the following option via the 'tweak' button:

Cleaning engine: 'automatically try to unregister objects prior to deletion'

IMPORTANT: Before letting AdAware delete malware, write down on a piece of paper exactly where the malware is stored. You will need to delete those directories after AdAware has done its work.

microsoft.public.security.virus: Re: is lavasoft recommended

After running AdAware, run it again, this time using the option 'select drives/folders to scan'. Click on 'select'. Scan your entire hard drive. Also do the following:

Empty your IE cache and your other temporary file folders, eg:
c:\windows\temp (if using Windows 98) or C:\Documents and Settings\<>name>\Local Settings\Temp (the path to your temp folder will change depending on your name) – sometimes programmes can be hidden in there – watch out for mysterious *.exe files or *.dll files in those folders.

Go to IE Tools, Internet Options, Temporary Internet Files {Settings Button}, View Objects, Downloaded Programme Files. Check for unusual objects there.

--

Hyperlinks are used to ensure advice remains current

Sandi – Microsoft MVP since 1999 (IE/OE)

<http://inetexplorer.mvps.org/>

apm.des wrote:

> Is lavasoft a reliable spyware removal source. i don't
> want to compound my computer problems by downloading
> a "fix" that will create more of the same problems (pop
> ups, default web pages, slow moving internet connections
> etc.).
>
> Thanks for any help.